BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

(19)日本国特許庁（ＪＰ）　(12)**公開特許公報（Ａ）**　(11)特許出願公開番号
特開2002－342106
（P2002－342106A）
(43)公開日　平成14年11月29日(2002.11.29)

(51)Int.Cl.⁷	識別記号	ＦＩ		テーマコード（参考）
Ｇ０６Ｆ　11/00		Ｇ０６Ｆ　9/06	６６０Ｎ	５Ｂ０７６
9/455		9/44	３１０Ｄ	

審査請求　未請求　請求項の数22　ＯＬ　（全 16 頁）

(21)出願番号　特願2001－345236(P2001－345236)

(22)出願日　平成13年11月９日(2001.11.9)

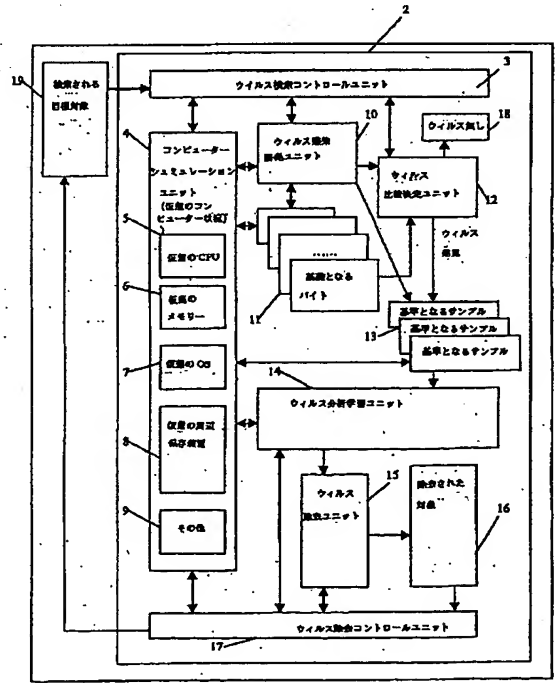
(31)優先権主張番号　０１１１７７２６．８
(32)優先日　平成13年４月29日(2001.4.29)
(33)優先権主張国　中国（ＣＮ）

(71)出願人　501436975
ベイジン　ライジング　テクノロジー　コーポレーション　リミテッド
中華人民共和国　100080　ベイジン　ハイディアン　ディストリクト　フォングアン　チュンストリート　ナンバー22　ホンケプラザ　13階
(74)代理人　100085028
弁理士　西森　浩司

最終頁に続く

(54)【発明の名称】　既知や未知のコンピュータウィルスの検索・駆除方法

(57)【要約】　（修正有）
【課題】　既知や未知のコンピュータウィルスの検索・駆除方法を提供する。
【解決手段】　ウィルスが存在する仮想のコンピュータ環境を作成し、感染を誘発するために複数のバイトを提供し、検索すべき目標対象をロードし、検索されるべき目的対象をアクティブにし、目的対象に付着していた可能性のあるウィルスを誘引して複数の対象を感染させると共に、実際に感染した基準サンプルを生成させ、アクティブにするステップで処理した後の複数の対象と、もともと提供された感染されるべき複数の対象とを比較し、変化があるかどうかを調べて、目標対象はウィルスを含んでいたかどうかを決定する。更に、生成した基準サンプルを分析することにより学習し、ウィルスに関する情報や知識を抽出し、ウィルスを駆除すると共に、ウィルスによって変更されたキー情報を、該ウィルスに関する情報や知識や、感染したバイトに対してウィルスが行った修正に基づき修正する。



【特許請求の範囲】
【請求項１】　コンピュータウィルス検索･駆除方法であって、
コンピュータウィルスが存在する仮想のコンピュータ環境をコンピュータ内にシュミレーションとして作成するステップと、
ウィルス感染を誘発するためにコンピュータウィルスによって感染されるべき複数の対象すなわちバイトを提供するステップと、
シュミレーションとして作成された仮想コンピュータ環境に検索すべき目標対象をロードするステップと、
シュミレーション作成された仮想コンピュータ環境内にある検索されるべき目的対象をアクティブにし、前記目的対象に付着していた可能性のあるウィルスを誘引して感染されるべき複数の対象を感染させると共に、実際に感染した基準サンプルを生成させるステップと、そして、
前記アクティブにするステップで処理した後の複数の対象と、もともと提供された感染されるべき複数の対象とを比較し、変化があるかどうかを調べて、もし変化があれば検索されるべき目標対象はウィルスを含んでいた、また、変化がなければ目標対象はウィルスを含んでいなかったと決定するステップと、
を含んでなるコンピュータウィルス検索・駆除方法。
【請求項２】　請求項１に記載のコンピュータウィルス検索･駆除方法において、
更に、生成した基準サンプルを分析することによりウィルスから学習し、ウィルスを分析すると共に、検索されるべき目標対象がウィルスを含んでいると決定されたらウィルスに関する情報や知識を抽出するステップと、そして、
ウィルス本体を除去することにより感染した対象からウィルスを駆除すると共に、ウィルスによって変更されたキー情報を、該ウィルスに関する前記情報や知識に基づき、また、前記感染した対象、すなわち、バイトに対してウィルスが行った修正に基づき修正するステップと、
を含んで構成されてなるコンピュータウィルス検索･駆除方法。
【請求項３】　請求項１又は２に記載のコンピュータウィルス検索･駆除方法において、
前記コンピュータシュミレーションステップは、
中央処理ユニット（CPU）のシュミレーション作成指示によって、CPUをシュミレーションで作成するステップと、
オペレーションシステム（OS）によって提供された様々なサービス及び様々なデータ構造をシュミレーションで作成することによってOSをシュミレーションするステップと、
保存空間及びシュミレーションされたハードディスクやフロッピィディスク等を含む様々な周辺保存装置の構造をシュミレーションで作成することによって周辺保存装置をシュミレーションするステップと、そして、
シュミレーションされたメモリスペースを発生させ、分配し、管理することによってメモリをシュミレーションするステップと、
を呼び出し且つ実行する機能的ファンクションを提供するステップを含んで構成されてなるコンピュータウィルス検索･駆除方法。
【請求項４】　請求項３に記載のコンピュータウィルス検索･駆除方法において、
検索されるべき目標対象は、異なる大きさ、異なるタイプのウィルスを誘発する内容及び種々の感染条件を持つ全ての種類のバイト、例えば、DOS COMタイプのウィルスを誘発するDOS COMタイプ用DOSファイルタイプのバイト、DOS ブートセクタタイプのウィルスを誘発するシュミレーション作成されたDOSブートセクタ、マクロウィルスからなるウィルスを誘発するWORDファイルタイプのバイト等を含んで構成されてなるコンピュータウィルス検索･駆除方法。
【請求項５】　請求項４に記載のコンピュータウィルス検索･駆除方法において、
異なる大きさや内容を持つ複数のバイトが、出来るだけ検索されるべき目標対象に付着したウィルスの感染条件を満たすように、所定のウィルスタイプについて供給されてなるコンピュータウィルス検索･駆除方法。
【請求項６】　請求項５に記載のコンピュータウィルス検索･駆除方法において、更に、時間や日付に敏感なウィルスを誘発するために仮想の時計や日付を発生させるシステム時計をシュミレーションで作成するステップを含んで構成されてなるコンピュータウィルス検索･駆除方法。
【請求項７】　請求項６に記載のコンピュータウィルス検索･駆除方法において、
前記OSシュミレーションステップが、DOS,WINDOWS（登録商標）,UNIX（登録商標）のためのOSの一つをシュミレーションで作成するステップを含んで構成されてなるコンピュータウィルス検索･駆除方法。
【請求項８】　請求項２に記載のコンピュータウィルス検索･駆除方法において、
前記ウィルス駆除ステップにおいて、ウィルスは、感染したホスト対象、すなわち、ウィルスを持っていると判断された検索されるべき目標対象からオリジナルの目標対象を再保存するように仮想的に動作し、しかる後、該ウィルスは駆除されることを特徴とするコンピュータウィルス検索･駆除方法。
【請求項９】　請求項３に記載のコンピュータウィルス検索･駆除方法において、
前記周辺保存装置シュミレーションステップは、メモリの中に仮想ハードディスクをシュミレーションで作成する小さなメモリ領域を割り当てると共に、該仮想ハード

ディスクは、通常のものと同じ構造、すなわち、セクタ番号、トラク番号及びシリンダ番号によって特定される三次元空間、主ブートセクタ及び０トラックの対応する空セクタ、隣のブートセクタ、ファイル位置テーブル（FAT）、ルートディレクトリ領域、そして、必要なシステムファイル並びにウィルスを誘発するバイトファイルを含んでいることを特徴とするコンピュータウィルス検索･駆除方法。

【請求項１０】　請求項３に記載のコンピュータウィルス検索･駆除方法において、

前記周辺保存装置シュミレーションステップは、メモリの中に仮想フロッピィディスクをシュミレーションで作成する小さなメモリ領域を割り当てると共に、該仮想ハードディスクは、通常のものと同じ構造、すなわち、ブートセクタ、ファイル位置テーブル（FAT）、ルートディレクトリ領域、そして、必要なシステムファイル並びにウィルスを誘発するバイトファイルを含んでいることを特徴とするコンピュータウィルス検索･駆除方法。

【請求項１１】　コンピュータウィルスの検索・駆除のための一般的なコンピュータシステムを含むコンピュータシステムであって、

コンピュータウィルスが存在する仮想のコンピュータ環境をコンピュータ内にシュミレーションとして作成するコンピュータシュミレーションユニットと；ウィルス感染を誘発するために提供されたコンピュータウィルスによって感染されるべき複数の対象すなわちバイトと；シュミレーションとして作成された仮想コンピュータ環境に検索すべき目標対象をロードする制御ユニットと、

シュミレーション作成された仮想コンピュータ環境内にある検索されるべき目的対象をアクティブにし、前記目的対象に付着していた可能性のあるウィルスを誘引して感染されるべき複数の対象を感染させると共に、実際に感染した基準サンプルを生成させるウィルス感染誘引ユニットと、

前記ウィルス感染誘発ユニットで処理した後の複数の対象と、もともと提供された感染されるべき複数の対象とを比較し、変化があるかどうかを調べて、もし変化があれば検索されるべき目標対象はウィルスを含んでいた、また、変化がなければ目標対象はウィルスを含んでいなかったと決定するウィルス存否決定ユニットと、

を含んでなるコンピュータウィルス検索・駆除システム。

【請求項１２】請求項１１に記載のコンピュータウィルス検索･駆除システムにおいて、さらに、

生成した基準サンプルを分析しウィルスがあると判断されたらウィルスに関する情報や知識を抽出するウィルス分析・学習手段と、そして、

ウィルス本体を除去することにより感染した対象からウィルスを駆除すると共に、ウィルスによって変更されたキー情報を、該ウィルスに関する前記情報や知識に基づき、また、前記感染した対象、すなわち、バイトに対してウィルスが行った修正に基づき修正するウィルス駆除ユニットと、

を含んで構成されてなるコンピュータウィルス検索･駆除システム。

【請求項１３】　請求項１１又は１２に記載のコンピュータウィルス検索･駆除システムにおいて、

中央処理ユニット（CPU）のシュミレーション作成指示を行うCPUシュミレーションユニットと、

オペレーションシステム（OS）によって提供された様々なサービス及び様々なデータ構造をシュミレーションで作成するOSシュミレーションユニットと、

保存空間及びシュミレーションされたハードディスクやフロッピィディスク等を含む様々な周辺保存装置の構造をシュミレーションで作成する周辺保存装置シュミレーションユニットと、そして、

シュミレーションされたメモリスペースを発生させ、分配し、管理するメモリシュミレーションユニットと、

を含んでなり、前記各ユニットは、呼び出されることにより利用可能で且つメモリ空間に割り当てられており、現実のCPU、OS、周辺保存装置からは独立している機能的ファンクションを含んでなることを特徴とするコンピュータウィルス検索･駆除システム。

【請求項１４】　請求項１３に記載のコンピュータウィルス検索･駆除システムにおいて、

検索されるべき目標対象は、異なる大きさ、異なるタイプのウィルスを誘発する内容及び種々の感染条件を持つ全ての種類のバイト、例えば、DOS COMタイプのウィルスを誘発するDOS COMタイプ用DOSファイルタイプのバイト、DOS ブートセクタタイプのウィルスを誘発するシュミレーション作成されたDOSブートセクタ、マクロウィルスからなるウィルスを誘発するWORDファイルタイプのバイト等を含んで構成されてなるコンピュータウィルス検索･駆除システム。

【請求項１５】　請求項１４に記載のコンピュータウィルス検索･駆除システムにおいて、

異なる大きさや内容を持つ複数のバイトが、出来るだけ検索されるべき目標対象に付着したウィルスの感染条件を満たすように、所定のウィルスタイプについて供給されてなるコンピュータウィルス検索･駆除システム。

【請求項１６】　請求項１５に記載のコンピュータウィルス検索･駆除システムにおいて、更に、

時間や日付に敏感なウィルスを誘発するために仮想の時計や日付を発生させるシステム時計シュミレーションユニットを含んで構成されてなるコンピュータウィルス検索･駆除システム。

【請求項１７】請求項１６に記載のコンピュータウィルス検索･駆除システムにおいて、

前記OSシュミレーションユニットが、DOS,WINDOWS,UNIXのためのOSの一つをシュミレーションすることを特徴と

するコンピュータウィルス検索･駆除システム。
【請求項１８】　請求項１２に記載のコンピュータウィルス検索･駆除システムにおいて、
前記ウィルス駆除ユニットは、ウィルスが感染したホスト対象、すなわち、ウィルスを持っていると判断された検索されるべき目標対象からオリジナルの目標対象を再保存するように動作し、しかる後、該ウィルスは駆除されることを特徴とするコンピュータウィルス検索･駆除システム。
【請求項１９】　請求項１３に記載のコンピュータウィルス検索･駆除システムにおいて、
前記周辺保存装置シュミレーションユニットは、メモリの中に仮想ハードディスクをシュミレーションで作成する小さなメモリ領域を割り当てると共に、該仮想ハードディスクは、通常のものと同じ構造、すなわち、セクタ番号、トラク番号及びシリンダ番号によって特定される三次元空間、主ブートセクタ及び０トラックの対応する空セクタ、隣のブートセクタ、ファイル位置テーブル（FAT）、ルートディレクトリ領域、そして、必要なシステムファイル並びにウィルスを誘発するバイトファイルを含んでいることを特徴とするコンピュータウィルス検索･駆除システム。
【請求項２０】　請求項１３に記載のコンピュータウィルス検索･駆除システムにおいて、
前記周辺保存装置シュミレーションユニットは、メモリの中に仮想フロッピィディスクをシュミレーションで作成する小さなメモリ領域を割り当てると共に、該仮想ハードディスクは、通常のものと同じ構造、すなわち、ブートセクタ、ファイル位置テーブル（FAT）、ルートディレクトリ領域、そして、必要なシステムファイル並びにウィルスを誘発するバイトファイルを含んでいることを特徴とするコンピュータウィルス検索･駆除システム。
【請求項２１】　請求項1～１０のいずれかに記載の方法のステップをコンピュータが実行するようにしたプログラムをコンピュータ読み込み可能に記録したコンピュータ記録媒体。
【請求項２２】ネットワーク伝達を経由して請求項1～１０のいずれかに記載の方法のステップをコンピュータが実行するようにした伝送媒体。
【発明の詳細な説明】
【０００１】
【発明が属する技術分野】本発明はコンピュータウィルスを検索し除去する（つまり捜索して駆除する）ソフトウェアの分野に関わり、特に、未知のウィルスの検索･駆除方法、それを実行する検索･駆除システム、記録媒体及びこのウィルス撃退ソフトウェアを保存し伝達するための伝送媒体に関わる。
【０００２】
【従来の技術】長い間、コンピュータを使う人を困らせるコンピュータウィルスは大きな問題であった。感染性、自己増殖性、破壊性というコンピュータウィルスの特徴のため、データの損失や改変、ファイルに損傷を与えたり、ソフトウェアを破壊したり、などコンピュータウィルスはコンピュータのユーザを恐れさせて来た。人々はそれらを検索･駆除するために様々なウィルス撃退ソフトウェアを使ってきた。
【０００３】今までのところ、一般的に使われてきたウィルス撃退ソフトウェアは既知のウィルス、つまり既知の様々なウィルス、従って、その特徴コードがすでに知られているウィルスのみを検索･駆除してきた。この場合において、ウィルスを持っている可能性のあるファイルは、ウィルスの特徴コードによって検索され、探される。いったん特徴コードが見つけられたら、そのファイルは感染していると決定され、ウィルスを駆除しにかかる。しかしながら、この方法は、未知の種類のウィルスは検索できなかった。ウィルス分析装置によって新しいウィルスが分析され発見された後でしか、特徴コードは得られない。それゆえ新しいウィルスは特徴コードが従来のウィルス撃退ソフトウェアに加えられるまで認識･検索されない。
【０００４】コンピュータウィルスの出現以来、その固有値を検索することによって検出してきた。つまり新しいウィルスが発見されたら、ウィルス分析装置がその固有値としてのウィルスプログラム本体から特徴的な一又は複数の特徴コードからなるクラスタ（塊）を抽出し、しかる後、ウィルス検索ソフトはファイル中にウィルスの固有値の存在を検索することによってファイルが感染しているかどうかを調べる。しかし、ウィルス撃退技術は過去十年でそれなりの進歩を遂げてきたが、ウィルス検索の方法が、ウィルス検索ソフトウェアに基づいている点では変わりがなかった。固有値検索方法（すなわちウィルス検索ソフトウェア）の致命的な欠点は、もしウィルスが発見されたら、ウィルス分析装置によってウィルス認識ライブラリに特徴コードが加えられ、ウィルス検索ソフトウェアはおなじ種類のウィルスを認識できる。逆の言い方をすれば、ウィルス検索ソフトウェアはいつもウィルスに遅れをとっており、ソフトウェアがウィルスに対して効果を発揮するようにするためには、その前に、ウィルス分析装置によってウィルスが分析されねばならない。
【０００５】未知のウィルスを検索できる従来のウィルス撃退技術、例えば、広域スペクトル検索方法、発見的検索方法などは、従来の古典的なウィルスの特徴コードに基づき、経験的に対象が感染しているかどうか、目標対象（ターゲットオブジェクト）が疑いのあるコードを持っているかどうかを、仮想マシーン上でウィルスに対し検索すべきターゲットオブジェクトのコードで作動することによって判断する。例えば、いくつかの国内、海外のウィルス撃退会社は、未知のウィルスを検索するた

めの方法を開発してきた。そのすべてはディスクに書き込んだり、ファイルに書き込んだりするようなウィルスの特徴的な方法を要約すると言うおなじ考えに基づいていて、目標対象の特徴コードを検索する。これらの方法は、実は、挙動上の特徴を定義付けるもので、帰納法的ウィルス検索方法又は発見的ウィルス検索方法と呼ばれる。

【0006】このような方法は、未知のウィルスを検索でき、警告を鳴らすことができるが、しかし効果が少なく、誤報や未報告の可能性も高い。これには二つの理由がある。ひとつは、ウィルス攻撃の方法が多様で数え上げることができない程あると言うことである。二つ目は、ウィルスによる攻撃方法が、複数のソフトウェアツールと同じくシステムに対して合法で、それゆえそれらを識別することが難しい。この種の方法を用いて、未知ウィルスのいくつかは、検索し・警告することができる。しかしながら、高い誤報率のためこれらの方法はユーザに不必要な懸念をもたらす。そして致命的な欠点はウィルスを検索できるけど、ウィルスを駆除できないと言うことにある。もし対象がウィルスによって攻撃されたら、ウィルス撃退ソフトウェアの品質が高められるまで、コンピュータをシャットダウンしなければならない。さらに目標対象が（ファイル、ブートセクタ、メモリなど）感染しているかどうか、を確定できず、“感染した可能性がある”事を告げるに過ぎない。今まで、ウィルス撃退製品はウィルス特徴ライブラリ（データベースやコードベース）なしに未知のウィルスを駆除したり既知のものを駆除したりすることはできなかった。

【0007】

【発明が解決しようとする課題】従来のウィルス撃退ソフトウェアの上記の問題に鑑み、本発明の目的は、未知や既知のウィルスを効果的に検索・駆除する方法・システム、記録媒体及び伝送媒体を提供する。未知のウィルスを効果的に検索する問題を解決するようにウィルスの存在を検索するためにウィルスの感染性を主に利用する。これにより、ほとんどの未知のウィルスを検索・駆除できる。これにより、人手で分析されて初めて、ウィルスを検索・駆除できるという状況を完全に変えるであろう。本発明は未知のウィルスを早期に検索・駆除でき、それにより、情報やデータを壊すウィルスの可能性を大幅に減らすことができる。ほとんどの未知・既知のウィルスに対する人手による分析を不要とするため、複数の労力とお金が節約される。

【0008】

【課題を解決するための手段】本発明は、コンピュータウィルスが存在する仮想のコンピュータ環境をコンピュータ内にシュミレーションとして作成するステップと、ウィルス感染を誘発するためにコンピュータウィルスによって感染されるべき複数の対象すなわちバイト（おびき寄せのための対象物）を提供するステップと、シュミレーションとして作成された仮想コンピュータ環境に検索すべき目標対象をロードするステップと、シュミレーション作成された仮想コンピュータ環境内にある検索されるべき目的対象をアクティブにし、前記目的対象に付着していた可能性のあるウィルスを誘引して感染されるべき複数の対象を感染させると共に、実際に感染した基準サンプルを生成させるステップと、前記アクティブにするステップで処理した後の複数の対象と、もともと提供された感染されるべき複数の対象とを比較するステップと、そして、変化があるかどうかを調べて、もし変化があれば検索されるべき目標対象はウィルスを含んでいた、また、変化がなければ目標対象はウィルスを含んでいなかったと決定するステップと、を含んでなるコンピュータウィルス検索・駆除方法を提供する。

【0009】本発明に係るコンピュータウィルス検索・駆除方法は、更に、生成した基準サンプルを分析することによりウィルスから学習し、ウィルスを分析すると共に、検索されるべき目標対象がウィルスを含んでいると決定されたらウィルスに関する情報や知識を抽出するステップと、そして、ウィルス本体を除去することにより感染した対象からウィルスを駆除すると共に、ウィルスによって変更されたキー情報を該ウィルスに関する前記情報や知識に基づき、また、前記感染した対象、すなわち、バイトに対してウィルスが行った修正に基づき修正するステップを含む。

【0010】本発明はコンピュータウィルスの検索・駆除のための一般的なコンピュータシステムを提供するもので、コンピュータウィルスが存在する仮想のコンピュータ環境をコンピュータ内にシュミレーションとして作成するコンピュータシュミレーションユニットと；ウィルス感染を誘発するために提供されたコンピュータウィルスによって感染されるべき複数の対象すなわちバイト（おびき寄せのための対象物）と；シュミレーションとして作成された仮想コンピュータ環境に検索すべき目標対象をロードする制御ユニットと、シュミレーション作成された仮想コンピュータ環境内にある検索されるべき目的対象をアクティブにし、前記目的対象に付着していた可能性のあるウィルスを誘引して感染されるべき複数の対象を感染させると共に、実際に感染した基準サンプルを生成させるウィルス感染誘引ユニットと、前記アクティブにするステップで処理した後の複数の対象と、もともと提供された感染されるべき複数の対象とを比較し、変化があるかどうかを調べて、もし変化があれば検索されるべき目標対象はウィルスを含んでいた、また、変化がなければ目標対象はウィルスを含んでいなかったと決定するウィルス存否決定ユニットと、を含んでなるコンピュータウィルス検索・駆除システムを提供する。

【0011】本発明に係るコンピュータウィルス検索・駆除システムは、更に、生成した基準サンプルを分析することによりウィルスから学習し、ウィルスを分析する

と共に、検索されるべき目標対象がウィルスを含んでいると決定されたらウィルスに関する情報や知識を抽出するウィルス分析学習ユニットと、そして、ウィルス本体を除去することにより感染した対象からウィルスを駆除すると共に、ウィルスによって変更されたキー情報を該ウィルスに関する前記情報や知識に基づき、また、前記感染した対象、すなわち、バイトに対してウィルスが行った修正に基づき修正するウィルス駆除ユニットとを含む。

【００１２】本発明はさらにコンピュータに上述のコンピュータ駆除方法の各ステップを実行させるようにしたコンピュータ読込可能な記録媒体を提供する。さらに、本発明はコンピュータに上述のコンピュータ駆除方法の各ステップを実行させるようにしたネットワーク伝送を経由した伝送媒体を提供する。

【００１３】

【発明の実施の形態】コンピュータウィルスのもっとも大切な特徴である感染性のためにコンピュータウィルスはそう名づけられた。もし、プログラムに感染性があったら、それはウィルスを持っていると決定される。それゆえ、プログラムの感染性を認識することによってウィルスを認識することが最も効果的な方法である。しかしながら、ウィルスの感染性により、感染性を認識する事は、ウィルスを何らかの対象に感染させることを意味する。もし決定が実際の状況で実行されたら、それはウィルス検索の間にウィルスが拡散していることを意味する。だから検索されるべき目標対象が感染しているかどうかを証明するために仮想環境において、実行されなければならない。本発明はウィルスの感染性を利用し、ウィルスを持っている疑いのある対象をコンピュータウィルスが存在する仮想のコンピュータ環境内に置き、再生産し、それをアクティブにし誘引してバイトに感染させる。さらに様々なウィルスは目標対象の大きさ、内容などのような特定の感染状況を必要とすることもあるので、本発明は異なる大きさ、内容を含むバイト対象を含む全ての種類のバイトを提供する。例えば、format.comやsort.com等のファイルがDOS COMタイプのウィルスを誘引するのに使われる。Debug.exeやlable.exe等のファイルがDOS EXEタイプのウィルスを誘引するのに使われる。フロッピィディスクブートセクタ、ハードディスクブートセクタやハードディスクの主ブートセクタはDOS BOOTタイプのウィルスを誘引するためにシュミレーションされる。そして、notepad.exeやword.exe等のファイルがWINDOWS PEタイプのウィルスを誘引するのに使われる。等々。異なるバイト対象ができる限りウィルスの必要条件を満たすために使われる。

【００１４】本発明は仮想コンピュータ環境中にあるウィルスの検索・駆除・報告・検索のための新しい技術に係るもので、行動・結果に従うウィルス撃退方法の一種である。本発明はウィルスの再生・拡散が認識される全てのプロセスにおいて、実際のコンピュータ環境をシュミレーションするための仮想コンピュータ環境を使う。同時にウィルスの再生や拡散の手順を観察し、ウィルスの感染方法を学習する。感染過程を逆に辿ることによりそのようなウィルスを駆除する方法が提供される。以下は細かい説明である。まずウィルスが存在し再生産される仮想環境が確立され、検索されるべき目標対象は仮想環境に置かれる。二番目に、疑いのある対象がアクティブにされる。もし本当にウィルスを持っていたら仮想環境は感染されたものとなる。様々な操作が仮想環境内のバイトに対して行われ、できる限りウィルスが感染するように誘引する。つまりウィルスの再生及び感染の実験は仮想環境でなされる。もしバイトがウィルスに感染していたら、検索されるべき目標対象はウィルスを持っていると言うこととなり、ウィルスによって感染したバイトは基準サンプルとなる。三番目に、もし前の再生ステップや感染の実験が成功したら、基準サンプルはウィルス分析装置の代わりのプログラムによって分析され、ウィルスの検索・駆除のために必要な情報が基準サンプルから引き出される。四番目に、プログラムの基準サンプルの分析から得られる情報はウィルスを駆除するためにウィルスを持つ感染した目標対象に当て嵌められる。

【００１５】図1は本発明に係るコンピュータウィルス検索・駆除のためのコンピュータシステムの一実施態様におけるブロック図である。図1に示されているように、一般的なコンピュータシステム1はコンピュータによって実行される本発明に係るウィルス検索・駆除ユニット２を含む。コンピュータシステム1は一般的なCPU、メモリ、OS、周辺保存装置（ハードディスク、フロッピィディスク、など）（図1には示されていない）を含む。ウィルス検索・駆除ユニット２の全体のプログラムはコンピュータシステム1内のCPUによって実行される。コンピュータシステムはさらに目標対象１９を含む。この目標対象１９は、コンピュータシステム２内のハードディスクやフロッピィディスクのブートセクタにあるファイル、及び、ウィルスを持っている可能性のあるインターネットを通してダウンロードされ且つ伝送されるファイル及びデータである。

【００１６】図1に示されているように、ウィルス検索・駆除ユニット２は、検索されるべき目標対象１９をシュミレーションとして作成されたコンピュータ環境に入力し、全てのウィルス検索構成要素のプロセスを管理するためのウィルス検索コントロールユニット３と；ウィルスが再生され、拡散する仮想コンピュータ環境として、シュミレーション作成された全コンピュータシステムを作るコンピュータシュミレーションユニット４、すなわち仮想のコンピュータと；ウィルス感染を誘引するための一又は複数の基準バイト（すなわち、コンピュータウィルスに感染した可能性のある目標対象）と；検索されるべき目標対象１９を仮想コンピュータ４にロード

し、オペレーションを実行し、基準バイト１１を用いて、検索されるべき目標対象１９によって保持されていた可能性のあるウィルスを基準バイト１１及び仮想ハードディスク、フロッピィディスクやシュミレーション作成されたコンピュータ環境の同様のものに感染させると共に、感染された基準サンプル１３を生成するウィルス感染誘発ユニット１０と；そして、仮想ハードディスク、フロッピィディスク、シュミレーション作成されたコンピュータ環境の同様のものがウィルス誘発ステップの前後で変わったかどうかを調べ、感染後の基準サンプル１３と感染前の基準バイト１１とを比較し、変化があるかどうかを決定し、もし変化があるなら、検索されるべき目標対象はウィルスを含んでおり、そうでなければウィルス１８はないと決定する比較・ウィルス存否決定ユニット１２と；を含んで構成されている。

【００１７】前述のシュミレーション作成されたコンピュータシステムは、仮想のCPU５、仮想のメモリ６、仮想のOS７、仮想の周辺保存装置８（ハードディスク、フロッピィディスクなど）及びシステム時計のようにウィルスの生存、再生、拡散のために必要とされるシステム構成手段９の他の部分を含んでいる。

【００１８】ウィルス検索・駆除ユニット２のウィルス駆除部分は、全ウィルス駆除コンポーネントの処理を制御するのに使用されるウィルス駆除制御ユニット１７と；基準バイト１１と感染した基準サンプル１３とから分かるウィルス感染により引き起こされた修正を分析し、且つ該ウィルスについての知識を学習するウィルス分析学習ユニット１４と；そして、ウィルス分析学習ユニット１４から得られた知識を基にウィルスを適当に排除又は駆除すると共に、ウィルスが駆除された対象１６を生成するウィルス駆除ユニット１５と；を含んでいる。駆除後の対象１６は、検索されるべき入力目標対象１９上にウィルス駆除制御ユニット１７により上書きするのに使用することができ、それにより、ウィルスを除去する。

【００１９】本発明の好ましい実施形態によると、ウィルス検索・駆除ユニット２とウィルス駆除制御ユニット１７は上記全てのウィルス検索・駆除プロセスを監視するために単一のコントロールユニットに統合することができる。

【００２０】コンピュータシュミレーションユニット４によって作られた仮想のコンピュータ環境は仮想のマシーン５（仮想のCPU）、仮想のＯＳ７、仮想の周辺保存装置８、仮想の周辺メモリ６などを含む。簡単に言えば、ウィルスの存続に必要とされる全てのコンピュータの構成手段はシュミレーション作成される。ウィルスを持っている可能性のある対象は理論的にウィルスによって感染してきたものであろう。ウィルスを持っているかもしれない対象は仮想環境に置かれ、適当な状況の下でアクティブにされる。

【００２１】仮想のCPU５はsoftcpu() と呼ばれる（ソフトウェアによって実行、シュミレーションされたCPU）。Softcpu()は実際のCPUによる指示の解釈プログラムである。それは実際のCPUのようにプログラムを解釈し実行し、それぞれの行のコードを理解でき、それらを正確に解釈、実行できる。理論的にsoftcpu()は実際のCPUができる全てのコードやプログラムを実行、解釈でき、どんな状況の下でも同じように全ての指示を解釈できる。実際のCPUが作用する全ての対象は（BIOSチップやディスク）本物であるのに対し、仮想のCPUが作用する対象（BIOSチップやディスク）は仮想のものである。

【００２２】それに加え、softcpu()は実際のCPUの指示を解釈するための単なる機能手段で、それはアセンブル言語、C言語や他の言語で書かれるものである。本発明の好ましい一実施形態においては、汎用性、維持性を考慮してC言語で書かれている。

【００２３】もしインテルコンピュータのウィルスを検索する場合、softcpu()がインテルのCPUをシュミレーションとして作成することであろう。もしマッキントッシュのコンピュータのウィルスを検索する場合、マッキントッシュのCPUをシュミレーションとして作成することであろう。

【００２４】全てのプログラムは特定のＯＳで動作するものであるが、ウィルスも同様である。仮想のＯＳ7はウィルスが動作するＯＳをシュミレーションとして作成する。仮想のＯＳ７は仮想のDOSのためのＯＳやWINDOWS 95のための仮想のＯＳ、UNIXのための仮想ＯＳなどのようなウィルスのために必要とされる複合的なＯＳを含む。本発明の一実施形態において効果を高めるために、仮想のＯＳ７はウィルスを動作するためにＯＳの必要な要点だけをシュミレーション作成する。

【００２５】DOSのウィルスのために、DOSのための仮想のＯＳが選ばれる。WINDOWS 95のウィルスのためにはWINDOWS９５のための仮想のＯＳが選ばれる。

【００２６】本発明に係るコンピュータシュミレーションユニット4は、ハードディスクやフロッピィディスクのような仮想のコンピュータ保存装置８を含む。仮想コンピュータ環境においては、検索されるべき対象のプログラム中に有る周辺保存装置への全ての書き込みや読み込みは仮想のものである。これは、仮想のプログラムが動いているときに引き起こされるディスク中のファイルやデータへの感染及び損傷は仮想ディスク中の感染及び損傷だと言うことを意味する。

【００２７】本発明の一実施形態において、仮想のコンピュータ周辺保存装置8は、コンピュータシュミレーションユニット４と呼ばれる機能手段又はプログラムユニット8を含んでおり、それにより、仮想のハードディスクを作る。仮想のコンピュータ周辺装置８の主な機能は、メモリの中に必要とされる大きさの領域を割り当て、特定の要求に従って、該メモリ領域に仮想ハードデ

ィスクをシュミレーションで作成することである。仮想ハードディスクは、通常のものと同じ構造、すなわち、セクタ番号、トラク番号及びシリンダ番号によって特定される三次元空間、主ブートセクタ及び０トラックの対応する空セクタ、隣のブートセクタ、ファイル位置テーブル（FAT）、ルートディレクトリ領域、そして、必要なシステムファイル（例えば、IO.SYS,MSDOS.SYS、COMMAND. COMがDOSシステムのために必要とされる）、並びにテスト用のバイトファイル（すなわち、DOSEXE.EXE,DOS COM.COMがDOSファイルタイプのウィルスのために必要とされるファイル）を含んでいる。本発明の検索・駆除システムに使われる仮想ハードディスクの中のデータは10キロバイトから数百キロバイトの大きさのメモリ領域のみしか占めない。これに対して、普通のハードディスクは数メガバイトから数ギガバイトの記憶容量がある。それらのほとんどは本発明によるシステムでは使われない。だから本発明の一実施形態において、数メガバイトから数ギガバイトの大きさを持つハードディスクをシュミレーションで作成するためには、メモリサイズは10キロバイトから数百キロバイトのみが必要とされるに過ぎない。大容量のハードディスクをシュミレーションするために本システムではほんの少しのメモリしか使わないため、このシステムに必要とされるハードディスクは一般的なコンピュータによって実現可能である。さらに、検索・駆除ステップの間、本物のハードディスクはアクセスされず、且つ仮想ハードディスクは、実際は小さいメモリ領域であるため、処理スピードは速く、時間は節約される。これに加え、仮想ハードディスクはメモリの単なる一部分で、本物のディスクは感染も損傷も受けない。メモリの物理的な特徴は破壊されてはおらず、ユーザシステムには無害である。

【００２８】本発明のさらにこの好ましい一実施形態においては、ユニット8がハードディスクをシュミレーションするために使う場合、世界的構造である可変Hard_Disk_Strucを予め定義することができ、それにより、空ディスク、システムファイル及びバイトファイルを記録したディスク等のシュミレーション作成されたハードディスクをコントロールする。

【００２９】仮想の装置8はまた必要なサイズのメモリ領域を主として割り当てることによりフロッピィディスクをシュミレーションで作成することができ、通常のものと同一の構造を有する仮想のフロッピィディスクをメモリ領域に構築する。通常のものと同一の構造には、ブートセクタ、ファイル位置テーブル（FAT）、ルートディレクトリ領域、そして、必要なシステムファイル（例えば、IO.SYS,MSDOS.SYS、COMMAND. COMがDOSシステムのために必要とされる）、並びにテスト用のバイトファイル（すなわち、DOSEXE.EXE,DOS COM.COMのようなファイル）を含んでいる。これらのすべてに必要なデータは１０キロバイトの大きさの領域を占めるに過ぎない。本発明の一実施形態において、世界的構造である可変floppy_disk_strucを予め定義することができ、それにより、空ディスク、ブートディスク、システムファイル及びバイトファイルを記録したフロッピィディスク等のシュミレーション作成された仮想フロッピィディスクをコントロールする。例えば、３６０キロバイト、７２０キロバイト、１．２メガバイト、１．４４メガバイト、などのサイズのフロッピィディスクを世界的なバリエーションとして作成することができる。

【００３０】同じようにして、他のＯＳのハードディスクやフロッピィディスクもシュミレーションで作成される。上記の柔軟な対応により、システム時間の消費が節約され、仮想の周辺装置8は作られたメモリ領域へ必要とされたデータをアップロードする。

【００３１】仮想のCPU５、仮想のメモリ６や仮想のOS７を含む上記全てのプログラムユニットは、プログラミング言語を知っている当業者によって実現することができる。それらには、CPUをシュミレーション作成するための全指示、メモリの管理及びアクセスの操作の全指示、全種類のデータ構造及びＯＳの機能サービスのため実行コードを含んでいる。これらの全ては市販のプログラム技術によって実行できるものであり、従って、本明細書ではその詳細を省略する。

【００３２】検索されるべき目標対象をアクティブにするため、目標対象に含まれるウィルスをアクティブにしてウィルスとしての行動を行わせる。例えば、目標対象が実行可能なバイナリファイル（DOS EXEファイル、DOS COMファイル、DOS BATファイル、WINDOWS NEファイル、PEファイル）である場合、実行するための手段をアクティブにする。目標対象が実行可能なマクロを持つWORDファイルのような文書ファイルの場合、マクロが実行されるような方法でそれをアクティブにする。

【００３３】上記の基準バイトは様々な日付や時間を含む仮想のシステム時計を含むもので、それにより、CIHウィルス（４月２６日、１３日の金曜日などに攻撃する）のように時間や日付に敏感なウィルスを誘発させる。図1に描かれているように、ウィルス検索・駆除プログラム２の検索部分は複数の基準バイト１１やバイトセットを含む、１セットの基準バイトを提供する。バイトはウィルスに感染した可能性のある既知の対象を参照する。本発明の一実施形態において、バイトはDOSのウィルスに対してはDOSプログラムであり、WINDOWS95のウィルスにはWINDOWS95のプログラムであり、WORDのウィルスのためにはWORDの文書である。以下、同様。バイトは目標対象がどんなものであれ、目標対象と同じタイプの実行可能な実在である。バイトは汚染されていなく、その大きさ、内容、構造、どのような行動をするのかの機能は既知であるのに対し、目標対象がウィルスを持っているかどうかは検索されるべき前には分からない。だからもしそれらがウィルスを持っていたら、それらの大

きさ、構造、どのような行動をするのかの機能は分からない。

【００３４】それに加え、上記のバイト１１は自由には選ぶことができず、しかし既知のウィルスに対して複数の実験によって該ウィルスに感染することが実証されている実行可能な実在でなければならない。それらの大きさ、内容はウィルスにとって、“おいしい”、つまりそれらは感染しやすいものである。もしバイトがウィルスに感染したら、そこから情報を引き出すことができる。つまりバイトは感染しやすい既知の実行可能な実在であり、バイトセットは感染しやすい全種類の１セットを構成する既知の実行可能な実在である。

【００３５】具体的には、本発明の一実施形態において、基準バイト１１は、例えば1キロバイトから６０キロバイトまでの（1キロバイト、２．５キロバイト、１２キロバイト、２０キロバイト、３０キロバイト、４０キロバイトのような）違う大きさを持った複数のバイトファイルを含むDOS COMタイプのバイトセットと；それぞれがJMP,CALL,MOV,XORであるべきバイトセット中のファイルの第一指示と；異なる時間、日付及びアトリビュートを持ち、それらに敏感な異なる種類のウィルスを誘発させるバイトセットの中のファイルと；を含んでいる。

【００３６】上記の基準バイトは、ファイルのヘッダの大きさが0x20, 0x200, 0x400、0x600、0x800で；ファイルの大きさが4KB,10KB,20KB,40KB,80KBで；その最後のページの大きさが0x00, 0x03, 0x80, 0x87, 0x100, 0x198で；そのリロケーションアイテムの数字が0x00, 0x01, 0x02, 0x04, 0x10であるが、完全にはリロケーションアイテムテーブルを占領しないもので； CS及びIPレジスタが様々な値のもので；プログラム本体のスタック位置がプログラム本体の冒頭、中間、末尾またはプログラム本体に隣接した位置である（プログラム本体の外）；ように構築することができる。

【００３７】上記の基準バイトは、MSDOS,PCDOS,WIN9Xシステムに対して、異なるバージョンのブートセクタのセットや主ブートセクタを含むブートタイプのバイトセットを含むように構築することができる。実際、それらは、WIN9X,PCDOS,DRDOSWIN9Xに対して、異なるバージョンのブートセクタや主ブートセクタを含む仮想のハードディスクやフロッピィディスクであり、それにより、コンピュータシュミレーションユニット4によって作られるBOOTタイプのウィルスを誘発する。

【００３８】同じように上記の基準バイトは、異なる大きさ、タイプのWORD文書を含むMACROウィルスのためのバイトセットを含むように構築することができる、それにより、MACROウィルスを誘発し感染させる。

【００３９】図1に示されているように、ウィルス感染誘発ユニット１０は（ウィルスサンプル製造マシーンともよばれる）ウィルス感染を誘発するためのプロセスを遂行する上記全種類のバイトセットを使う機能ユニットで、従って、検索されるべきファイル及びその中に存在する可能性の有るウィルスを動作して、それにより、できる限りたくさん、基準ホストファイル（すなわち、上記の全バイト）に感染させる。そして、ウィルス認識ユニット１２は、ウィルスサンプル製造マシーン１０に感染したバイトがあるかどうか決定する。具体的には、ウィルス認識ユニット１２は、検索されるべき目標対象をウィルス感染誘発ユニット１０中で動作させた後のバイトと動作させる前のバイトとを比較し、変化の有無を調査する。動作の前後でバイト変化がある場合、目標対象がウィルスを有している決定され、当該変化したバイトはウィルスサンプルとなる。つまり、もしウィルスサンプル製造マシーン１０がサンプル１３を作らなかったら、目標対象は汚染されてはいない。そうでないなら、目標対象はウィルスを含んでいて、ホストファイル（バイト）はウィルス駆除のための全ての情報を含む基準サンプルとなる。本発明の一実施形態において、上記仮想DOSシステムの上記仮想メモリにウィルスが存在したら、ウィルスサンプル製造マシーン１０は、実行し、開き、読み込み、閉じ、検索する等を通じて、DOSEXE,DOS COMタイプのバイトを動作させ、それによって、できる限りそのバイトに感染させる。感染又は修正があった場合、その目標対象は基準サンプルとなる。

【００４０】文書タイプのウィルスには、感染したバイトそれ自身が基準サンプルになる。しかし、ブートセクタタイプのウィルスには、ウィルスサンプル製造マシーン１０が、ウィルスによって変えられた仮想ハードディスクや仮想フロッピィディスクのブートセクタの情報に従って、基準サンプルを作る。

【００４１】前記基準サンプル１３は、ウィルスの感染した基準バイト又はホストを参照する。基準ホストは、ウィルス分析装置によって既知とされる大きさ、内容、構造を持つ実行可能なボディであり、適当な感染状態の下でウィルスを持っていそうなものである。

【００４２】図1に示されているように、本発明の一実施形態においては、発明に係るウィルス駆除部分のウィルス学習マシーン１４（基準サンプル分析装置とも呼ばれる）は、上記の基準バイト１１と作られた基準サンプル１３とを比較し、サンプルを分析し、ウィルスを駆除するために必要とされた情報やウィルスに関する全ての情報を抽出する。このプロセスは、ウィルス学習マシーンの学習プロセスと呼ばれる。ウィルス学習マシーンの学習プロセスは、人手による仕事をシュミレーションによって行うウィルス学習プロセスで特徴コードを使用しない。すなわち、特徴コードを用いてウィルスの駆除を行うものとは完全に異なるものである。基準サンプルからウィルス学習マシーンによって抽出される知識や情報は、ウィルスの大きさ；ホストファイル中のウィルスの位置；ウィルスが暗号化され且つ変態化しているかどう

か；ウィルスがホストを暗号化しているかどうか；ウィルスが駆除できない（除去のみによってできる）ほどひどい損傷を受けていないかどうか；ウィルスがホストを移動しているかどうか；ウィルスがホストの分節を連結しているかどうか；そして、ホスト対象のキー情報の価値や位置が修正されているかどうかなどを含む。

【００４３】例えばDOS COMタイプのウィルスには、ウィルス学習マシーン１４は２種類の知識を抽出する。一つ目はウィルスの大きさであり、二つ目はホスト対象のオリジナルの機能が統合されたままか、ウィルスによって損傷を受けているかどうかである。ウィルスの大きさを計算するために使われる計算法のひとつは、基準サンプルから基準バイト（ホスト）の大きさを引き算することである。該計算法により、それが終了する又は仮想コンピュータが停止するまでに、コンピュータシュミレーションユニット4によって作られた仮想コンピュータ環境中の基準サンプルに対しホスト対象のオリジナルの機能が動作したか否かが決定される。もし、プロセスの間に基準バイトのオリジナルの機能が現れたら、ホスト対象のオリジナルの機能は統合されたままであった事を示し、そうでなければそれらは破壊されたのである。

【００４４】特徴コードを使う従来のウィルス駆除方法は、ウィルス分析装置に蓄積された既知ウィルスの特徴ライブラリにある情報（データやコード）によってウィルスを駆除する。しかし本発明に係るウィルス駆除ユニット１５は、人手による仕事をシュミレーションすると共に、既知ウィルスの特徴コードを使うこと無く、ウィルス学習ユニット１４によってリアルタイムに学習された知識に従ってウィルスを駆除するウィルス駆除ユニットである。ウィルスを駆除する基本理念は、“結んだ者がそれを解くことができる。”である。つまり、ウィルスサンプル製造ユニット１０及びウィルス駆除ユニット１４は、ウィルスの感染プロセスを学習し、感染結果（基準サンプル）を分析してウィルスのデータやアトリビュートを獲得する。ウィルスの特徴は感染し拡散する一方でそれ自身を隠蔽することにある。つまり、たいていのウィルスはホストのオリジナルの機能に損傷を与えることはなく、もしウィルス駆除ユニット１５が実際にウィルスに対して実行しても、ウィルスはホスト対象を回復させ、そして、ウィルス駆除ユニットはウィルスによって回復されたホスト対象を汚染されていない対象としてディスクに救済してしまうこととなる（もし、対象がディスクの中とは異なる方法でメモリ内に存在する場合には、対応する変更を行うべきである）。ウィルスが回復した場合、ホスト対象は、ウィルス学習マシーンによって学んだウィルスのアトリビュートによって、判断されなければならない。例えば、本発明の一実施形態において、ウイルスによる自己復帰方法はウィルス駆除ユニット１５が感染の逆プロセスすなわち、ウィルス駆除の過程を推論する方法のひとつとなる。もし、ウィルス駆除マシーンがウィルスのデータ又はアトリビュートを十分に学習したなら、全てのアトリビュート又はデータを用いて元のホストのキー情報（ウィルスによって修正された情報）を計算し、ウィルスを駆除する。ウィルスについてのリアルタイムの学習やそれを用いてのリアルタイム駆除は、ウィルス駆除ユニット１５によって実現される。これは、全ての既知のウィルス撃退ソフトウェア製品に対して有利であるとは言えない。

【００４５】本発明の一実施形態において、ウィルス駆除ユニット１５がDOS COMタイプの普通のウィルスを駆除するプロセスは次のようである。まず、もし基準サンプルのオリジナルの機能が統合されていない場合、ウィルスを持っているファイルは削除され、そうでなければプロセスは次のステップへと進む。検索されるべきDOS COMタイプの目標ファイルを仮想コンピュータ環境にロードし、仮想CPU中のプログラムセグメントレジスタCSの値がプログラムセグメントプレフィックスレジスタのアドレスと等しくなり且つIPレジスタの値が0x0100になるまで実行する。三番目に、駆除された目標対象の大きさを計算する。駆除されたDOS COMファイルの大きさは、感染したDOS COMファイルの大きさからウイルスの大きさを引くことにより計算する。四番目に、仮想メモリの内容を（CS:IP）から（CS:IP+駆除されたDOS COMファイルのサイズ）へと蓄積し直すことにより駆除された目標DOS COMファイルをファイルとして発生させる。

【００４６】もし、上記ウィルス学習マシーン１４がウィルスについての知識を得ることができなかった場合、又は、ウィルス学習ユニット１６が、ホストのオリジナルの機能が損傷を受けたと判断した場合、目標対象は削除される。

【００４７】図２、図３及び図４は、それぞれ、本発明の一実施形態に係るウィルス駆除方法のプロセスの流れ図である。流れ図中の全てのステップは図１のそれぞれの処理ユニットで実行されものので、それにより、ウィルス検索・駆除プロセスの全体を構成する。図２に示されているように、まず検索されるべき目標対象１９は、ハードディスク、フロッピィディスク、インターネット(ステップS101)を通じて入力されたデータから読み込まれる。そして、目標対象がウィルスを持っている可能性のある対象かどうかの決定がなされる（ステップS102）。ウィルスを持っている可能性のある対象は、理論的にウィルスに感染させるために利用できるが、ウィルスを持っている必要は必ずしもない。ウィルスを持っている可能性のある対象は、「.exe」、「.com」、「.bat」、「.doc」NEやPEタイプのファイル、ディスクのブートセクタや主ブートセクタのような実行可能な実在でなければならない。実行不能の実在、例えば、「.txt」は、ウィルスを持つことは不可能である。

【００４８】もし、ステップS102において、対象がウィルスを持っている可能性が有る対象と決定されたら、ウ

ィルスを検索し駆除するために次のプロセスに進む。もし、目標対象がウィルスを持つことができないものである場合、例えば、「.txt」のような実行不能の対象である場合、目標対象は汚染されていないと決定される。もし、対象が未知なら、対象は未知のものであると報告される。

【００４９】ステップS103において、コンピュータシュミレーションユニット４は、仮想のCPU、仮想のOS、仮想の周辺保存装置（ハードディスクやフロッピィディスク）、仮想のメモリ、仮想のシステム時計を含む仮想のコンピュータ環境を作り、それにより、内部にウィルスを持っている可能性のある対象を仮想上実行する。ステップS104において、ウィルスに感染し得る複数のバイトを提供する。バイトは、上記のファイルタイプのバイトセットや仮想ハードディスクや仮想フロッピィディスクにおけるブートセクタタイプのバイトセットを含む。ステップS105において、目標対象１９を仮想コンピュータ環境内に置く。ステップS106において、目標対象に付着していた可能性の有るウィルスがアクティブにされ、つまり、仮想コンピュータ環境及びバイトファイルが感染するように誘発する。一方、ステップS107において、バイトが感染したかどうかの決定がなされる。一方で、ステップS108において、仮想のコンピュータ環境が感染したかどうかの決定がなされる。すなわち、仮想のメモリ、仮想のハードディスクやフロッピィディスクが感染したかどうかの決定がなされる。もし、ステップS107において、バイトが感染していると判断されたら、プロセスは図３のステップS111に進む。そうでなければ、目標対象は汚染されていないと報告される。もし、ステップS111において、仮想のコンピュータ環境がウィルスを持っていると決定されたら、プロセスは図３のステップS110に進む。できる限り多くの操作を仮想コンピュータ環境内でバイトに対して行い、それにより、できる限りそれらが感染するようにウィルスを誘発する。その後、感染したバイトがあるかどうかもう一度判断するためにプロセスはステップS107に戻る。

【００５０】図３に示されているように、ステップS111において、検索されるべき目標対象がウィルスを持っていると報告された場合、基準サンプルが作られ、さらに、DOSウィルスや、MACROウィルスやブートセクタウィルスのようなウィルスのタイプが分析される。しかる後、ウィルスを駆除すべきかどうか決定をユーザに促すためにプロセスはステップS112に進む。もし、目標対象は感染したという報告に対し、ユーザがウィルスを駆除することを必要としなかった場合、ステップS109において検索システムは終了する。そうでなければ、もしユーザがウィルス駆除を必要としていたら、プロセスはステップS113に進む。

【００５１】ステップS113において、仮想のコンピュータ環境において作られた全基準サンプルが抽出される。そして、ステップS114において、これら抽出された基準サンプルはウィルス学習マシーン１４によって分析される。すなわち、その主部分が基準サンプルのオリジナルの機能（基準バイトのオリジナルの機能）が変えられたかどうかを判断する。ステップS115において、基準ホストのオリジナル機能の統合性が調べられる。もし、統合されていなかったら、プロセスはステップS116に進む。そうでなければプロセスはステップS120に進む。

【００５２】ステップS116において、もし、ホストのオリジナル機能がウィルスによって復帰できないほど破壊されたら、ホストは削除されねばならなくなるであろう。ステップS117において、ユーザが感染したファイルを削除することを望んでいるか否かが問われる。もしイエスなら、ファイルは削除される（ステップS117）。そうでなければ、ウィルス駆除プロセスは終了する（ステップS119）。

【００５３】図４に示されているように、ステップS120において、ウィルス学習ユニット１４はウィルスに関する全ての知識を学習し、十分学習するまで、できるかぎりウィルスを駆除するために必要とされるキーデータ又はアトリビュートを得る。例えば、DOS COMウィルスについては、次の知識シーケンスで十分である；まず、ウィルスが暗号化されていないか、変態化されていないか、そして、その大きさが変えられていないか；二番目に、ウィルスの大きさ；三番目に、ウィルスがホストの初めの３バイトを変えていること；四番目に、ウィルスが存在するホストの初めのバイトがどこにあるか、である。

【００５４】しかる後、ステップS121において、ウィルス駆除ユニット１５は、検索されるべきホスト内のウィルス（ホスト対象）によって修正されたキーデータやアトリビュートを、ウィルス学習マシーン１４によって学習された知識によってサーチし計算する。例えば、DOS COMウィルスには次の情報である事が知られている；まず、ウィルスは暗号化又は変態化されていない、そして、その大きさは変えられないこと；二番目に、ウィルスの大きさ；三番目に、ウィルスがホストの初めの三バイトだけを変えていること；四番目に、ウィルスが存在しているホストの初めの三バイトがどこにあるかが既知であること；である（（ウィルス本体に対する）data_offset_in_virus）。従って、ウィルス駆除のためのステップは次のようになる。まず、ファイル中のウィルス本体の位置（virus_offset_in_file）は、目標対象の大きさ（file_size）からウィルスの大きさ（virus_size）を引き算することによって計算される;二番目に、ホストの最初の三バイトの位置（（ウィルス本体に対する）data_offset_in_virus）が計算され、それは（virus_offset_in_file）と（data_offset_in_virus）との合計に等しい；三番目に、ホストの初めの三バイトは（data_offset_in_virus）の位置における三バイトのデータによ

って置き換えられる；そして、四番目に、感染したファウルの最後の部分はウィルスの大きさのバイト分だけ最後から削除される；である。

【００５５】ステップS122において、ウィルスによって修正されたホスト情報のオリジナル値の計算が成功したかどうかの判断がなされる。もし成功していなかったら、ウィルス駆除のプロセスは失敗したのである（ステップS125）。そうでなければ、プロセスはステップS123に進む。

【００５６】ステップS123において、ウィルスによって修正されたファイルの大きさやファイルヘッダのデータなどの目標ファイル（ホスト対象）のデータやアトリビュートは再保存される。それゆえ、ウィルスは駆除される。

【００５７】ステップS124において、ウィルスの駆除が成功したと言う報告がなされる。しかる後、プロセスはステップS119に進み、ウィルス駆除プロセスは終了する。

【００５８】本発明に係る上記ウィルス検索・駆除方法及び全ての各ユニットは、普通のコンピュータ言語（C言語のような）を使って実現することができ、それにより、対応するソフトウェアをプログラムする。そして、そのようなソフトウェアは、普通のコンピュータで実行可能である；フロッピィディスクの中に保存され、それにより、販売され又は使用される；またはネットワーク又はインターネットを通して伝達又はダウンロードされ、そして、実行される。

【００５９】ソフトウェアによって実現される本発明に係るコンピュータウィルス検索・駆除の方法及びシステムは、コンピュータウィルスの基本的な特徴、すなわち、感染性という能力を利用するもので、それにより、ウィルスを検索し、ウィルスについての知識をリアルタイムで学習し且つ利用する。それは、従来の全てのウィルス撃退ソフトウェア商品よりも有利である。本発明はその特定の行動ではなく、その代わりに、その“結果”によってウィルスを特定する。従来のものは、「行動／結果による技術」と名づけられている。もちろん、本発明の方法も、ウィルスの行動やそれら行動の結果の両方を認識するし、その結果に従って、ウィルスを安全に駆除できる。しかし、本発明は、特定の個々の行動（ディスクへの書き込みなど）は調べず、従って、かなりの時間が節約され、スピードが速い。さらに、本発明は、実メモリの小さい領域のみを使って、ウィルスの生存や再生のための仮想コンピュータ環境を提供する。従って、十分早い処理スピードを有しており、最大限、ウィルスの感染を誘発する。

【００６０】本発明に係るコンピュータのシステム及び方法により、たいていの既知・未知のウィルスは、もはや人手による分析を必要とせず、また、ウィルスの特徴コードを用いずに駆除される；そして、同時に新しく出現したウィルスを見つけることができる；駆除することができるウィルスも限界がなく；そして、本発明に使われるウィルス撃退ソフトウェアはもはやウィルスに遅れをとることはなく、未知のウィルスを確実に検索・駆除できる。

【００６１】本発明は、好ましい実施形態に関して特に述べられているが、それは本発明の範囲を限定する意味ではない。本発明の精神や範囲から逸脱することなく、様々な変化や修正が可能であることは当業者によって理解されるであろう。それゆえ、発明の範囲は、添付した請求の範囲によって定義されるべきである。

【図面の簡単な説明】

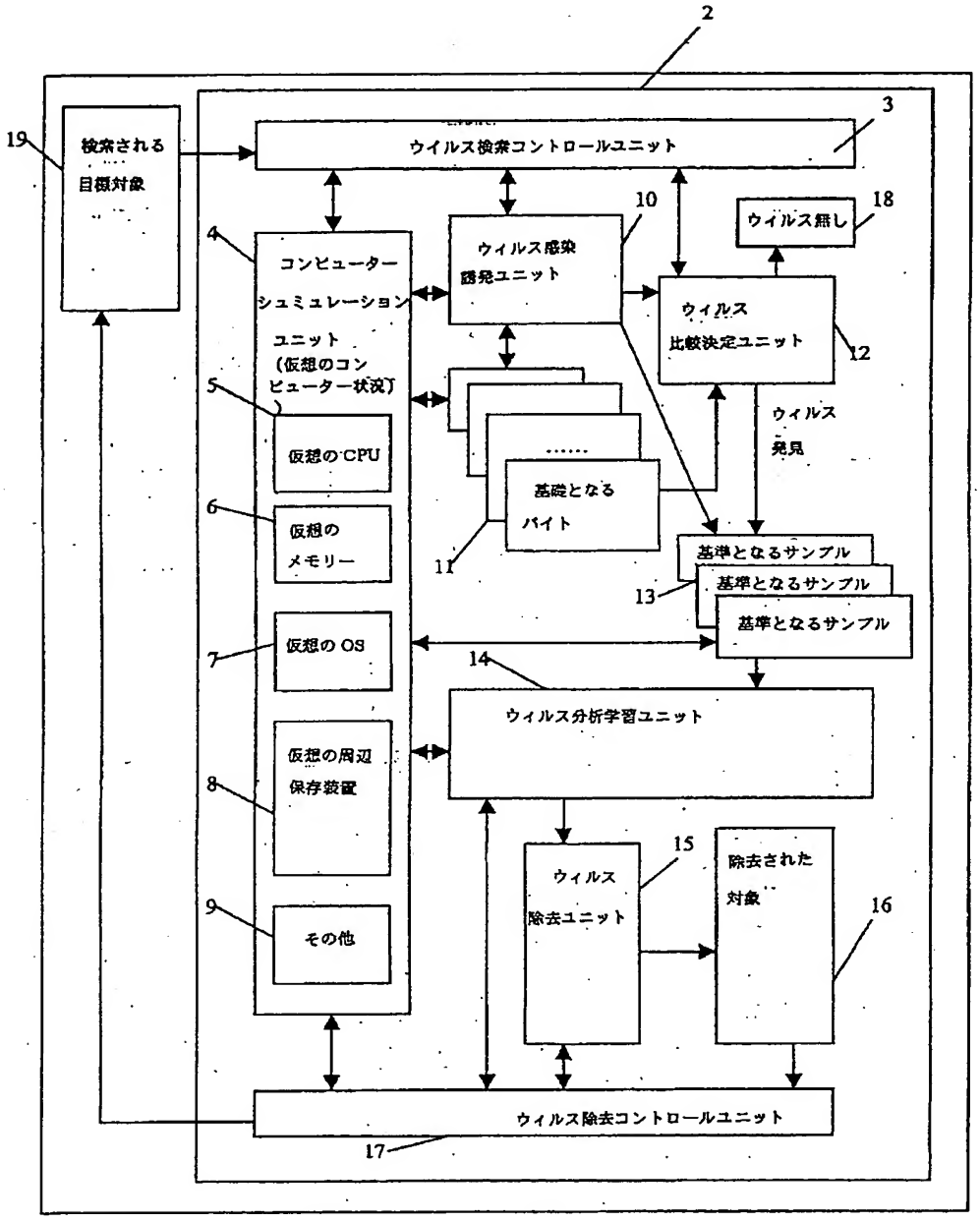
【図１】図1は本発明に係るコンピュータウィルスを検索・駆除するコンピュータシステムの枠組みを説明するためのブロック図である。

【図２】本発明に係るコンピュータウィルスを検索・駆除するための方法を示す流れ図である。

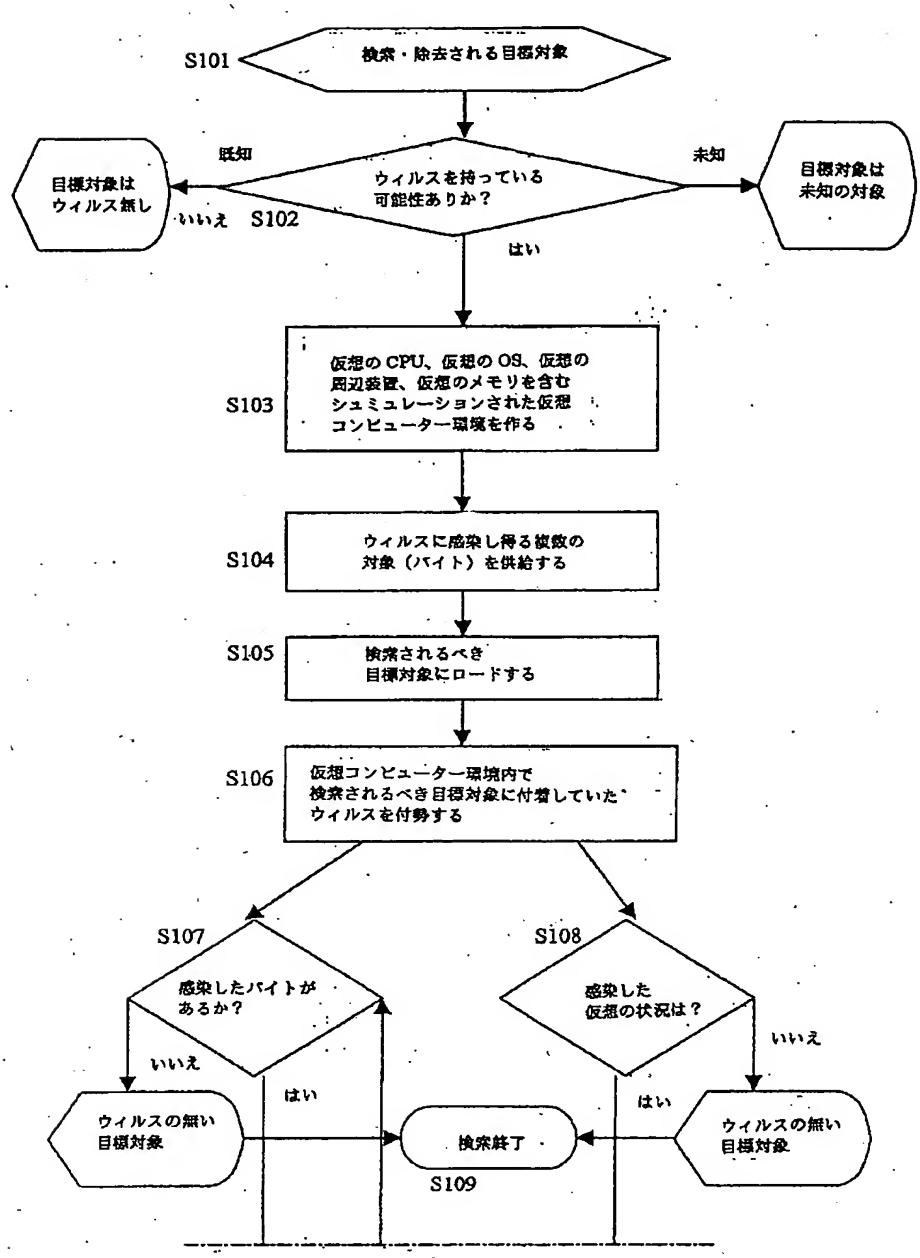
【図３】本発明に係るコンピュータウィルスを検索・駆除するための方法を示す流れ図である。

【図４】本発明に係るコンピュータウィルスを検索・駆除するための方法を示す流れ図である。

【図１】

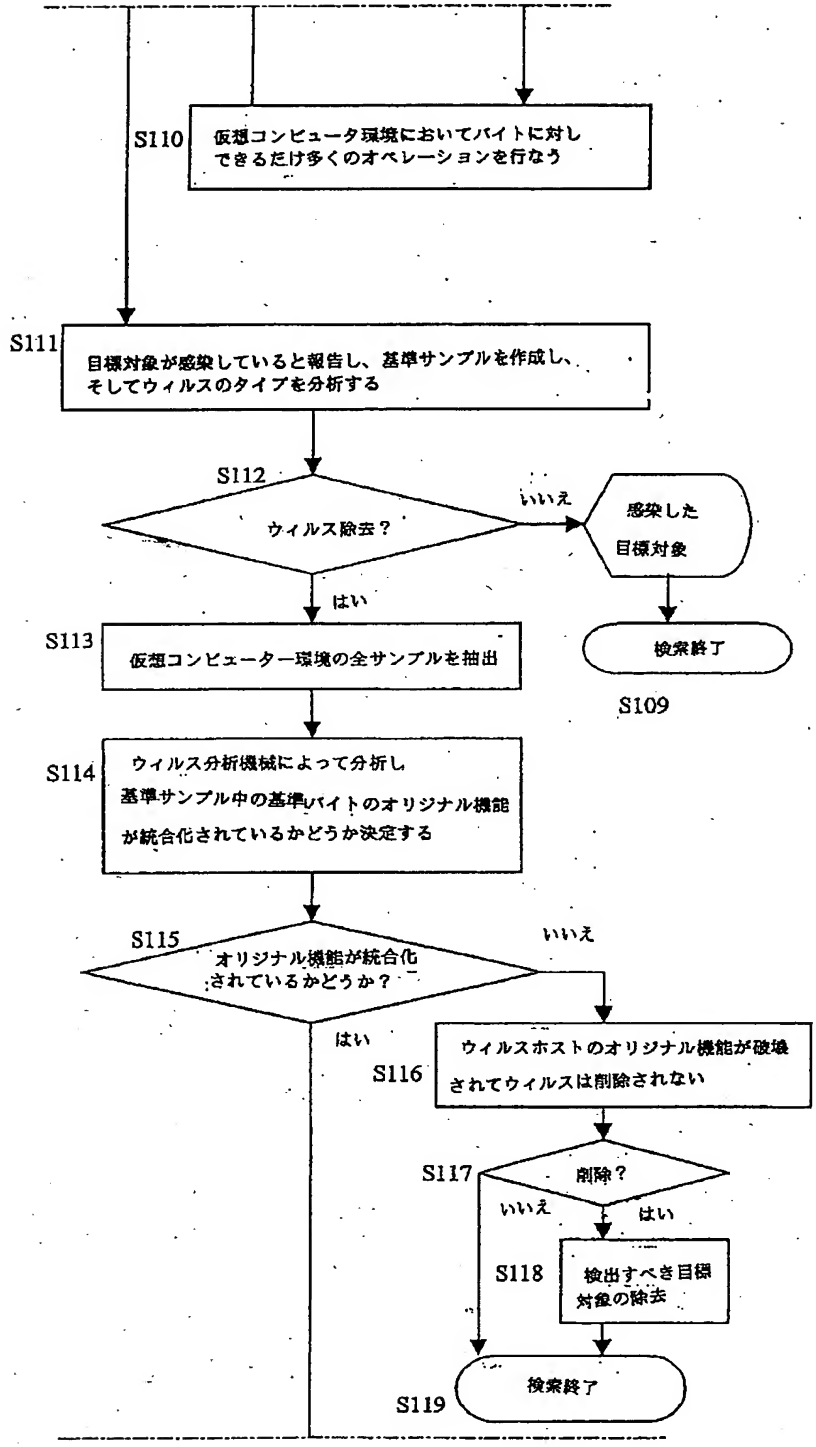

2
3
19
検索される
目標対象
ウイルス検索コントロールユニット
10
ウイルス感染
誘発ユニット
ウイルス無し
18
4
コンピューター
シュミュレーション
ユニット
（仮想のコン
ピューター状況）
ウイルス
比較決定ユニット
12
5
仮想のCPU
ウイルス
発見
6
仮想の
メモリー
基礎となる
バイト
11
基準となるサンプル
基準となるサンプル
13
基準となるサンプル
7
仮想のOS
14
ウイルス分析学習ユニット
仮想の周辺
保存装置
8
15
ウイルス
除去ユニット
除去された
対象
16
9
その他
ウイルス除去コントロールユニット
17

【図２】

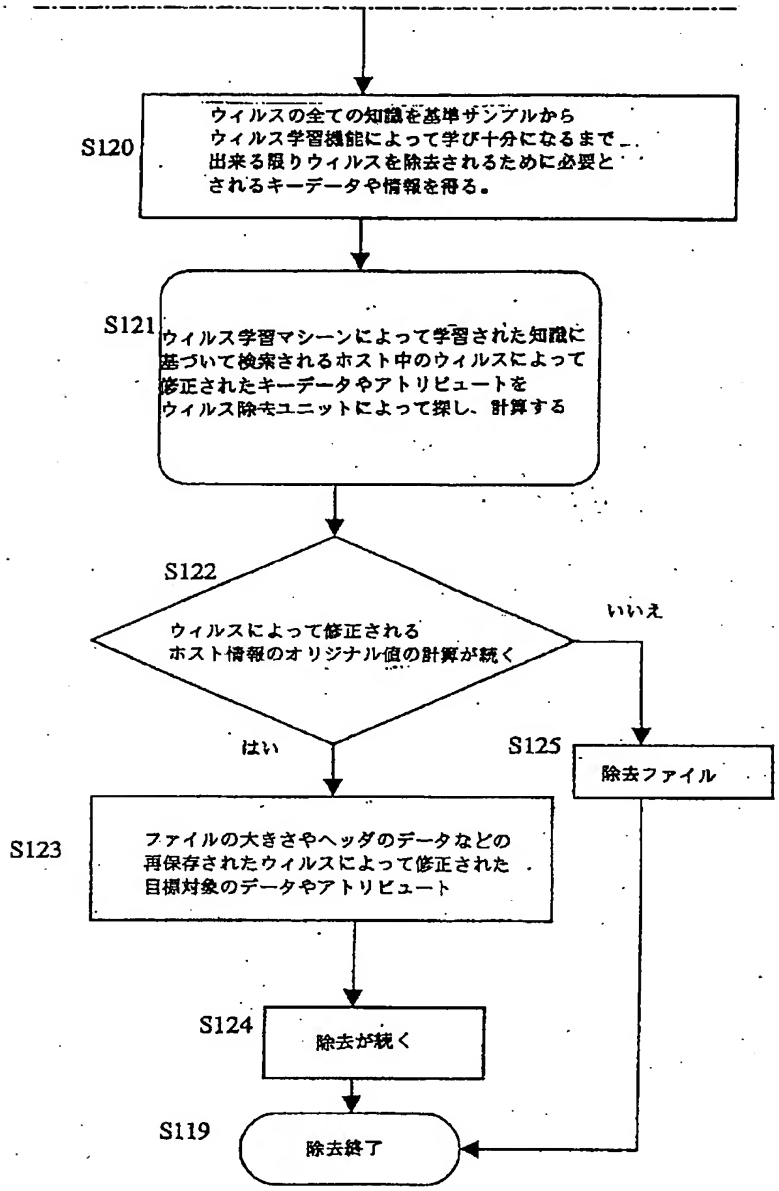

S101
検索・除去される目標対象
既知
未知
目標対象は
ウィルス無し
ウィルスを持っている
可能性ありか？
目標対象は
未知の対象
いいえ
S102
はい
S103
仮想のCPU、仮想のOS、仮想の
周辺装置、仮想のメモリを含む
シュミュレーションされた仮想
コンピューター環境を作る
S104
ウィルスに感染し得る複数の
対象（バイト）を供給する
S105
検索されるべき
目標対象にロードする
S106
仮想コンピューター環境内で
検索されるべき目標対象に付着していた
ウィルスを付勢する
S107
感染したバイトが
あるか？
S108
感染した
仮想の状況は？
いいえ
はい
いいえ
はい
ウィルスの無い
目標対象
検索終了
S109
ウィルスの無い
目標対象

【図３】

図３


S110
仮想コンピュータ環境においてバイトに対し
できるだけ多くのオペレーションを行なう
S111
目標対象が感染していると報告し、基準サンプルを作成し、
そしてウィルスのタイプを分析する
S112
ウィルス除去？
いいえ
感染した
目標対象
はい
検索終了
S109
S113
仮想コンピューター環境の全サンプルを抽出
S114
ウィルス分析機械によって分析し
基準サンプル中の基準バイトのオリジナル機能
が統合化されているかどうか決定する
S115
オリジナル機能が統合化
されているかどうか？
いいえ
はい
S116
ウィルスホストのオリジナル機能が破壊
されてウィルスは削除されない
S117
削除？
いいえ
はい
S118
検出すべき目標
対象の除去
S119
検索終了

【図４】



フロントページの続き

(72)発明者　タン　ハオミョウ
中華人民共和国　100080　ベイジン　ハイディアン　ディストリクト　フォングアンチュンストリート　ナンバー22　ホンケプラザ　13階気付

Fターム(参考)　5B076 FD08